EFFICIENT AND SECURE DISTRIBUTION OF INFORMATION WITHOUT THE NEED OF A CENTRAL ORGANIZING ENTITY

C. J. Gaughan* and J. L. Sagripanti, Dr. Sc.,
Edgewood Chemical Biological Center
APG-EA, MD, 21010

M. P. Bottiger
ITT Corporation
Abingdon, MD, 21009

G. Anderson
Drexel University Data Fusion Lab
Philadelphia, PA, 19104

ABSTRACT

In the pursuit of new research into the field of network sciences, we have chosen to focus on current logistical communication issues. The following research has been directed toward the application of basic swarm theory in managing data transfer securely over a dynamic network. The successful completion of this work will provide simple to compute solutions to currently intensive communication problems.

1. INTRODUCTION

1.1 Purpose

The success of a mission depends on efficient and secure distribution of tactical information. A medium independent network, which is able to securely transport information and adapt to changes in network connectivity and membership, will assist in making strategically important decisions. We propose a swarm based network, which provides efficient, stable, and secure delivery without the need of a central organizing entity.

1.2 Network Science

The pursuit of information on swarming behavior and networks is of particular interest to the field of Network Science. The Committee on Network Science for Future Army Applications of the National Research Council (NRC) recently released a report (NRC, 2006), which defined Network Science as "the study of network representations of physical, biological, and social phenomena leading to predictive models of these phenomena." They addressed the need for robust and secure networks stating, "There is a clear need to…design networked systems that are both robust to variations in the components (including localized failures) and secure against hostile intent." Furthermore, the NRC recommended that basic research on swarms and their applications be performed, with particular interest in the self-organizing and self-healing capabilities of a swarm, and that basic research on security and information assurance of networks be performed, with particular interest in "properties of networks that enhance survival".

2. THE SWARM NETWORK

2.1 Characteristics of a Swarm

The concept of swarming has been researched "using ants and other social insects as models". (Bonabeau and Theraulaz, 2006) Swarms have the unique characteristic of collective intelligence. A swarm may be governed by a few simple heuristics, but as a whole can carry out complex behavior well beyond the sum of its parts. They are self-organizing and when implemented correctly display the robustness, scalability, and flexibility of swarms observed in nature, e.g., ants (Bonabeau et al., 2000), termites, bees, etc. Furthermore, due to the innately dynamic nature of swarm networks, they are self-healing. Swarms can work cooperatively both to reestablish broken communication links, as well as redeploy in order to make up for lost members.

2.2 Peer-to-Peer Networks

Routing communication in any type of network is considered an NP hard problem (Chen et al., 2000). Peer-to-peer networks represent an exciting new method to use the cumulative resources of a networked system to achieve maximum information throughput in a distributed manner. These networks "are distributed systems based on the

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 NOV 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Efficient And Secure Distribution Of Information Without The Need Of A Central Organizing Entity	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Edgewood Chemical Biological Center APG-EA, MD, 21010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002075.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**4**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

concept of resource sharing by direct exchange between *peer* nodes (i.e., nodes having the same role and equal responsibility)" (Montresor et al., 2002). Despite the enticing potential advantages of harnessing the innate computing power of multiple discrete entities, challenges still remain.

2.3 Our Concept

Even though a distributed system removes many of the bottlenecks associated with traditional client/server paradigms, the network itself may still become unbalanced or generate hot spots. A solid load balancing algorithm is necessary to maintain maximum efficiency and proper data integrity. Another issue associated with any distribution scheme is validating the identity of any other peer node and assuring the integrity of data shared between any two locations.

To address these two concerns (solid load balancing and data integrity) we are proposing a peer-to-peer-based distribution system featuring a load balancing algorithm based upon the "Heatbugs" swarming simulation (also known as swarm intelligence (Kennedy et al., 2001)), combined with public key data encryption. We used this model as the basis for our data distribution algorithm.

2.4 Swarm Implementation

The Heatbugs swarm (Wilensky, 2004) is an example of using an adaptive biologically based algorithm to solve a real world minimization problem. In the simulation, each bug moves in a two-dimensional torus environment attempting to achieve an ideal body temperature. Each bug radiates heat into its world; this heat builds and radiates into space based upon predefined constants. In a communications network, each peer may connect to any other peer, but depending on the physical distance and number of routes involved there will be a cost associated with any transfer. This cost is analogous to the temperature in the Heatbug world, just as the number of connected peers will be analogous to the number of heat bugs in the environment. We used the information gathered from simulating our environment with a Heatbug-like algorithm to determine optimal data distribution and replication. Figures 1 shows the distribution in space of an example Heatbug simulation with 500 bugs, an ideal temperature range of 25° C to 52° C, a range of output heat of 13° C to 34° C, and a random-move-chance of 10% (this keeps the simulation from staying at equilibrium). The systems attempts to minimize the unhappiness of the Heatbugs (a plot of which is shown in Figure 2). At $t = 122.1$ clock cycles, the environment was heated up for 5 clock cycles, which produced a temporary decrease in the measure of unhappiness. Conversely, at $t = 166.4$ clock cycles, the environment was cooled down for 5 clock cycles, which produced a temporary increase in the measure of unhappiness.

Fig. 1 – Heatbug distribution in space

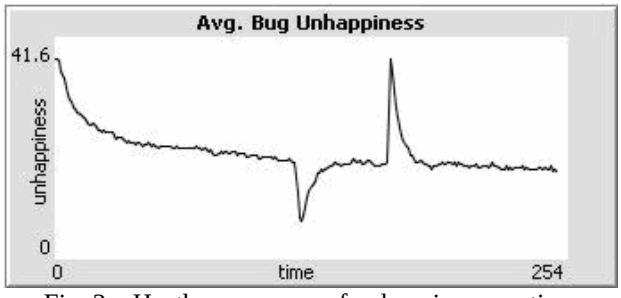

Fig. 2 – Heatbug measure of unhappiness vs. time

2.5 Security

We provide a security scheme that guarantees integrity, authenticity, and confidentiality. We first fragment files into reasonably sized blocks in order to reduce the overhead associated with the encryption/decryption process as well as take advantage of the parallelism in multi-processor computing systems. We employ a public key infrastructure (Rivest et al., 1977; ElGamal, 1985) (PKI) system in which the public keys are pre-distributed and use the Diffie-Hellman Algorithm (Diffie and Hellman, 1976) for inter-host negotiation of the symmetric key for the encryption of the blocks. The public and private keys are used for verification and validation of host identity and, to prevent man-in-the-middle attacks, they are used during the execution of the Diffie-Hellman algorithm.

3. Simulation Configuration

3.1 Assumptions

Our Swarm Network consists of n_e subscribed entities, each with data processing speed s_{p_i} where $i = 1,2,\cdots,n_e$. This model currently assumes that n_e is known at the start of the simulation, and in turn, that each entity is aware of the other. This implies that all entities share public key knowledge of the other as well as the fact that an entity knows which entity in the network has the data for which it wishes to request; however, this does not imply that it automatically knows the path to that entity Moreover, it assumes that no entities are lost during the simulation, no new entities subscribe to the network, and that all entities are transmitting the same type of data. The size of the data to be sent is represented as L_{Data} and is assumed to be the same for all transfers. The time necessary to recompile L_{Data} after a transfer is complete is dependent on s_{p_i} and is denoted as $t_{recompile}$. The cost is a function of

3.2 Simple Example

At its most basic, our implementation of the Heatbugs swarm can be modeled as a decision process. At every time instant of its existence in the simulation, an entity wishes to minimize its unhappiness; within our algorithm unhappiness is defined as a cost in time required to transmit information along a route between a requesting entity and a sending entity. With this goal in mind, an entity which is either requesting data or broadcasting data follows this process until its data load is completely transmitted:

1. Connect to each neighbor
2. Determine if neighbor knows entity with desired data/who requested data
3. Assess the cost of using the connection with that neighbor
4. Record state of the network at that instant
5. Transmit data using the connection with the least cost
6. Continue to transmit data until the cost of using the connection becomes greater than the cost of another neighboring entity as learned in Step 4 (Note: This is not necessarily still the same cost of transmitting using that connection)
7. Assess the cost of using the connection with the neighbor remembered to have a lower cost than the current connection
8. If Step 7 yields a better connection, then this connection is utilized until cycling back to Step 6
9. If Step 7 does not yield a better connection, continue to test the connection from lowest cost to highest cost as remembered from record of network
10. If Step 9 does not yield an alternative, cycle back to step 1

3.3 Encryption

To account for our encryption algorithm, we penalized the entities *w.r.t.* s_{p_i}. The PKI was taken into account when an entity was establishing communication links with its neighbors and determining the cost of using that connection (Steps 1-3 in the simplified version of our process). The Diffie-Hellman was factored in after a connection was established (Step 5), which means that the node had already made a decision on which node to pair up with in a transfer.

4. Conclusion and Future Work

Through the combination of cryptographic methods and a swarm-based load balancing algorithm, we have attempted to provide a unique solution to many current data transport issues involving the loss of connectivity, lack of security, or physical limitations of a single connection (e.g., speed of the connection). Ultimately, we have laid the framework for a simulation of efficient and secure distribution of tactical information for the warfighter.

Our simulation is currently in beta testing. Upon completion of version 1.0, we plan to extend our simulation in its next iteration to be able to

- handle entities not being aware of one another at the start of the simulation
- handle the loss of entities during the duration of a simulation
- handle variable length L_{Data}

REFERENCES

Alberto Montresor, Hein Meling, and Özalp Babaoğlu, "Messor: Load-Balancing through a Swarm of Autonomous Agents", Technical Report UBLCS-2002-11, September 2002, Department of Computer Science, University of Bologna.

A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. T. ElGamal, IEEE Transactions on Information Theory, 31(4), July 1985, pp: 469-472.

Committee on Network Science for Future Army Applications. Network Science, National Research Council. 2006.

E. Bonabeau and G. Theraulaz, "Swarm smarts," *Scientific American*, March 2006, pp. 82-90.

E. Bonabeau, M. Dorigo, and G. Theraulaz, "Inspiration for optimization from social insect behavior," *Nature*, vol. 406, pp. 39-42, July 2000.

J.C. Chen, C.S. Chen, B.J. Chen, M.Lay, L.Liu, B.Lee, S.Huang, W.Chang and D.Huang, “Application of Vehicle Routing Problem with Hard Time Window Constraints “, The 29th International Conference Computers and Industrial Engineering, Nov. 2000.

Kennedy J, Shi Y. and Eberhart R.C., “Swarm Intelligence”, Morgan Kaufmann Publishers, San Francisco, 2001.

New Directions in Cryptography. W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644-654.

R. L. Rivest and A. Shamir and L. M. Adelman. A Method For Obtaining Digital Signatures and Public-Key Cryptosystems. MIT/LCS/TM-82, 1977.

Wilensky, U. (2004). NetLogo Heatbugs model. http://ccl.northwestern.edu/netlogo/models/Heatbugs. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.